

UNITED STATES DISTRICT COURT

for the
Northern District of New York

In the Matter of the Search of)

(Briefly describe the property to be searched or identify the person by)
name and address)Devices seized from 818 Dennis Lane, Herkimer, New York)
13350, further described in attachment A.)
)
)

Case No. 5:22-MJ-593 (ATB)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A.

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1029
 18 U.S.C. § 1028A
 18 U.S.C. § 1343
 18 U.S.C. § 1349
 18 U.S.C. § 371
 18 U.S.C. § 1956

Offense Description

Access Device Fraud
 Aggravated Identity Theft
 Wire Fraud
 Wire Fraud Conspiracy
 Conspiracy
 Money Laundering

The application is based on these facts:

See affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Sydney Scannell, USSS Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone (specify reliable electronic means).

Date: 10/6/2022



Judge's signature

City and state: Syracuse, New York

Hon. Andrew T. Baxter

Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

SYDNEY SCANNELL, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of various electronic devices, further described in Attachment A, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. As detailed below, based on my training and experience, and the facts herein, my investigation shows that during or about September 2017, and continuing until the present, there is probable cause to believe that Valerie Aiello (“AIELLO”) and individuals associated with this investigation have committed violations aggravated identity theft (18 U.S.C. § 1028A); access device fraud (18 U.S.C. § 1029); wire fraud (18 U.S.C. § 1343); wire fraud conspiracy (18 U.S.C. § 1349); conspiracy (18 U.S.C. § 371); or money laundering (18 U.S.C. § 1956); structuring (31 U.S.C. § 5324) in the Northern District of New York. There is also probable cause to search the devices as more fully described in Attachment A (collectively, the “DEVICES”), for evidence, instrumentalities, contraband, and fruits of the offenses, further described in Attachment B.

3. I am a Special Agent (SA) with the United States Secret Service (USSS). I have been operating in that position since February 2, 2021. I am currently assigned to the Syracuse Resident Office. In that capacity, my duties include investigating federal criminal offenses committed in the Northern District of New York and elsewhere. I am responsible for

investigating crimes related to credit, debit, and identity card production and fraud, wire fraud, mail fraud, identity theft, the manufacture and possession of counterfeit currency, as well as financial crimes involving the use of digital technology.

4. I have received training regarding computer information security, various fraud and money laundering schemes, and computer fraud. I have conducted and assisted with investigations that have had an association with computer fraud and wire fraud, following the completion of the Special Agent Training Program of United States Secret Service at the James J. Rowley Training Center (JJRTC), located in Laurel, Maryland. Included within this training program, was cybercrime specific coursework, including the Basic Investigation of Computer and Electronic Crimes Program (BICEP). BICEP training was an 80-hour course consisting of understanding various computer operating systems to include Windows, Unix/Linux, and Mac OS X, and an understanding of how computers and accompanying systems are utilized in a variety of crimes. My training to become a USSS SA also included the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia. During my investigative career with the USSS, I have been exposed to numerous cases where electronic media, including computers, laptops, printers, scanners, and media storage devices (optical media drive such as CDs, removable flash drives, USB drives, and external hard drives, etc.) have been utilized in a variety of crimes. I am familiar with, and have participated in, many typical methods of investigation throughout my training to include interviewing subjects, victims, and witnesses, mobile and static surveillance, utilizing cooperating defendants and informants, the use of course authorized wire and electronic intercepts, utilizing undercover agents, obtaining search and seizure warrants with Assistant United States Attorneys (AUSA), and the use of Grand Jury subpoenas.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, officers, and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. This affidavit is made in support of an application for a warrant to search the following DEVICES, which were seized from the residence of the target of my investigation on February 8, 2022, for the evidence listed in Attachment B:

<i>Herkimer PD Item #</i>	<i>Device</i>	<i>Make</i>	<i>Model</i>	<i>Serial Number</i>
9	Desktop Computer	HP	White	4CI6100GMG
19	iPad	Apple	iPad	Unknown without device access
27	Laptop 1	HP	Presario F700	CNF4746S8N
28	Laptop 2	Samsung	RS40	HKGS93AB900793J
29a	USB 1	Sandisk	Cruzer	SDCZ60-032G
29b	USB 2	Sandisk	Cruzer	SDCZ6-4096RB
29c	USB 3	PNY	Black	N/A
29d	USB 4	Sandisk	Black Ultra	SDCZ48-064G
29e	USB 5	ONN	Gray	1003557

7. Each of the DEVICES were seized by the Herkimer Police Department and are currently held at the Herkimer Police Department headquarters at 120 Green St, Herkimer, NY 13350. The applied-for warrant would authorize the forensic examination of the DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. On or about February 11, 2022, the USSS received information from Herkimer Police Department Officers and Investigators regarding possible aggravated identity theft (18 U.S.C. § 1028A); access device fraud (18 U.S.C. § 1029); wire fraud (18 U.S.C. § 1343); wire fraud conspiracy (18 U.S.C. § 1349); conspiracy (18 U.S.C. § 371); or money laundering (18 U.S.C. § 1956); structuring (31 U.S.C. § 5324) on multiple accounts, amounting to a total loss of approximately \$108,000 by Signet Jewelers. By interviewing the victim and consulting with Herkimer Police Department, USSS Special Agents gathered evidence indicating Signet Jewelers and other retail stores fell victim to a fraudulent merchandise purchase and return scheme.

9. On or about July 13, 2021, Herkimer Police Department received a complaint of a grand larceny from Pete DANNER, Regional Loss Prevention Manager for Signet Jewelers. Signet Jewelers owns several jewelry companies, including Kay Jewelers, Jared Jewelers, Zale's, and others. As part of his employment, DANNER was made aware of possible fraudulent activity involving items purchased and returned online. These items were shipped to 818 Dennis Lane, Herkimer, New York 13350 (the "PREMISES") and the purchaser was listed as James DONNELLY. The purchaser placed three online orders for several pieces of jewelry from "Kay.com" from December 2020 to May 2021. DANNER advised that the purchaser would receive the orders at the PREMISES and eventually return the order. The purchaser's money

would be returned to the account for the full amount of the order. DANNER informed after the returns were received, Signet Jewelers discovered several of the items of jewelry that were returned were not the original jewelry that had been purchased. DANNER explained the purchaser returned replica jewelry pieces of much lower value than the originally purchased pieces. DANNER stated the purchaser did return some of the original pieces of jewelry. DANNER determined the purchaser received \$17,139.86 in returns for items that were not the original merchandise that was purchased.

10. On or about March 10, 2022, DANNER reviewed Signet Jeweler's records of purchases shipped and returned from the PREMISES and determined this scheme had been occurring since during or about 2017. DANNER documented a total of \$107,717.03 in refunds processed from online orders.

11. Based on the evidence gathered thus far and statements from witnesses, there is probable cause to believe AIELLO made numerous purchases of jewelry from "Kay.com" via electronic devices attached to the Internet, then returned fraudulent less expensive pieces of jewelry, keeping the originally purchased item, thus getting the money back as well. AIELLO works on these schemes at the PREMISES, has merchandise shipped to the PRESMISES and resides there.

12. The DEVICES are currently in the lawful possession of the Herkimer Police Department. They came into Herkimer Police Department's possession in the following way: On February 3, 2022, Herkimer Village Court Judge, Joanne Nitka, signed an application for search warrant for 818 Dennis Lane, Herkimer, New York 13350 for any Police Officer of the Village of Herkimer Police Department or any Police Officer of the State of New York to search and seize the following property: computers, computer peripheral devices, data storage devices, computer security devices, records and/or documents. On February 8, 2022, Herkimer Police Department

executed the search warrant and collected 49 items of evidence. Some of these items are the DEVICES. While the Herkimer Police Department might already have all necessary authority to examine the DEVICES, I seek this additional warrant out of an abundance of caution to be certain that an examination of the DEVICES will comply with the Fourth Amendment and other applicable laws.

13. The DEVICES are currently in storage at Herkimer Police Department headquarters located at 120 Green St, Herkimer, NY 13350. In my training and experience, I know that the DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICES first came into the possession of the Herkimer Policed Department.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal

calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. I submit that if a computer or storage medium was found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how

computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium that was in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, where, when, why, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed

or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Lastly, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner.

f. The DEVICES may have been used as instrumentalities of the crime because it is used as a means of committing the criminal offenses. The computer is also likely to be a storage medium for evidence of the crime(s). From my training and experience, I believe that the DEVICES used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

17. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. Generally, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for this examination is indefinite. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time. As explained above, because the warrant calls for forensic electronic evidence, it is necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored.

b. Technical requirements. The DEVICES can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations, therefore, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with specialized forensic tools and knowledge.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review

may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

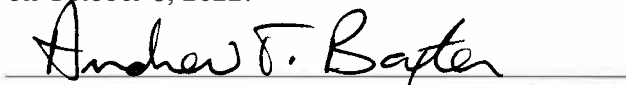
20. Therefore, I respectfully request that the attached warrants be issued for the locations and items outlined in Attachment A, and authorizing the search and seizure of the items listed in Attachment B.

Respectfully Submitted,



Sydney Scannell
Special Agent
United States Secret Service

Subscribed and sworn to before me
on October 6, 2022:



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
ITEMS TO BE SEARCHED

The items to be searched are currently in the secure custody at Herkimer Police Department headquarters located at 120 Green St, Herkimer, NY 13350 and consist of the following:

- A white colored HP Desktop Computer with serial number 4CI6100GMG
- An Apple iPad with serial number unknown until the device may be accessed
- An HP Presario F700 Laptop with serial number CNF4746S8N
- A Samsung Laptop RS40 with serial number HKGS93AB900793J
- A black colored Sandisk Cruzer USB with serial number SDCZ60-032G
- A black colored Sandisk Cruzer USB with serial number SDCZ6-4096RB
- A black colored PNY USB
- A black colored Sandisk Ultra USB with serial number SDCZ48-064G
- A gray colored ONN USB with serial number 10003557

This warrant authorizes the forensic examination of each Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

Items of evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of aggravated identity theft (18 U.S.C. § 1028A); access device fraud (18 U.S.C. § 1029); wire fraud (18 U.S.C. § 1343); wire fraud conspiracy (18 U.S.C. § 1349); conspiracy (18 U.S.C. § 371); money laundering (18 U.S.C. § 1956); structuring (31 U.S.C. § 5324) (collectively, the “Specified Federal Offenses”):

1. Communications, photographs, text files, or any other records concerning use of credit cards, the acquisition of personal information to be used in furtherance of the fraud, and the planning and execution of the fraud scheme to use credit cards;
2. Any sales receipts or other documentation regarding the purchase, sale, or return of merchandise or consumer goods;
3. Communications, photographs, text files, or any other records concerning the authorization of credit card accounts created in various names, debit cards, or other access devices, or any account information associated with such devices or identification information;
4. Information tending to identify any co-conspirators, criminal associates, or others involved in a fraud scheme to steal account information, open access device accounts utilizing other identities, to structure and launder the proceeds of the merchandise return scheme;
5. Any material that is evidence of the state of mind of Valerie AIELLO or other potential co-conspirators in violating the Specified Federal Offenses;
6. Any available identifying information associated with the DEVICES;
7. Information tending to identify other facilities, storage devices, or services—such as email addresses, IP addresses, phone numbers, or evidence of paired devices—that may contain electronic evidence described in any of the preceding paragraphs;
8. Any and all notes, documents, records or correspondence, or other evidence, concerning the individuals who used or owned the DEVICES in or about September 2017 through the present;
9. Any passwords and encryption keys that may be necessary to access the DEVICES;
10. Any evidence of computer-forensic programs (and associated data) that are designed to eliminate data from the DEVICES;
11. All records pertaining to online purchases made by or involving AIELLO since in or about September 2017, including:

- a. bank records, checks, credit card bills, account information, and other financial records;
- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- d. Evidence of user attribution showing who used or owned the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.